

INFORMATION RECORDER, METHOD FOR VERIFYING AUTHENTICITY AND COMPUTER-READABLE RECORDING MEDIUM STORING PROGRAM TO ALLOW COMPUTER TO EXECUTE THE METHOD

2

Publication number: JP2000286839

Publication date: 2000-10-13

Inventor: KANAI YOICHI

Applicant: RICOH KK

Classification:

- international: G11B20/10; G06F3/06; G06F12/14; G09C1/00;
H04L9/32; G11B20/10; G06F3/06; G06F12/14;
G09C1/00; H04L9/32; (IPC1-7): H04L9/32; G09C1/00;
G11B20/10

- european:

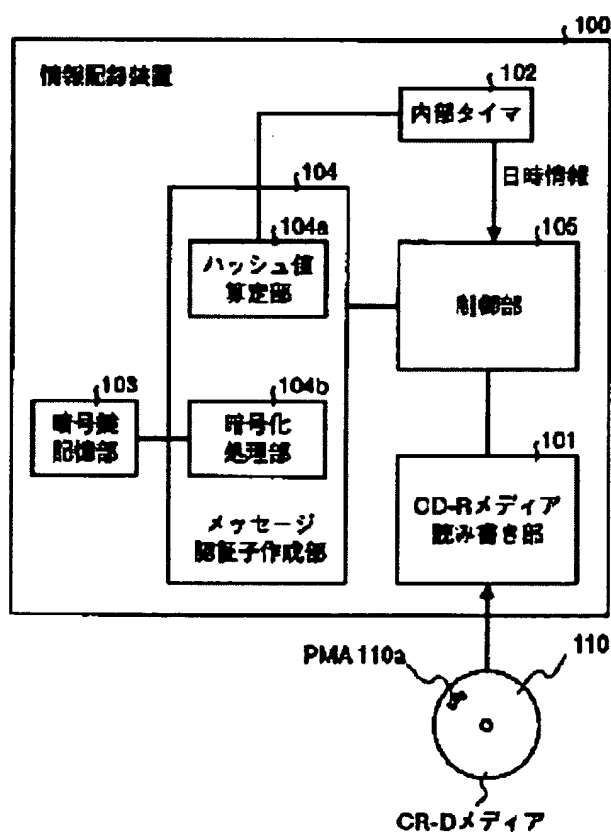
Application number: JP19990093850 19990331

Priority number(s): JP19990093850 19990331

Report a data error here

Abstract of JP2000286839

PROBLEM TO BE SOLVED: To provide an information recorder, a method for verifying authenticity and a recording medium by which a value of evidence of electronic data recorded on the recording medium can efficiently be enhanced. **SOLUTION:** A message authenticator generating section 104 generates a message authenticator based on media identification information specified to media such as a vendor ID, a drive ID and a disk ID stored in a PMA 110a, date and time information stored by an internal timer 102, a data recording position and electronic data and records the generated message authenticator to a CD-R medium 110 together with the electronic data.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-286839
(P2000-286839A)

(43) 公開日 平成12年10月13日 (2000. 10. 13)

(51) Int.Cl. ⁷	識別記号	F I	テームト [*] (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B 5 D 0 4 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 J 1 0 4
G 1 1 B 20/10		G 1 1 B 20/10	H 9 A 0 0 1

審査請求 未請求 請求項の数21 O L (全 12 頁)

(21) 出願番号 特願平11-93850

(22) 出願日 平成11年3月31日 (1999. 3. 31)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式
会社リコー内

(74) 代理人 100089118

弁理士 酒井 宏明

Fターム(参考) 5D044 BC05 CC04 DE39 DE49 EF05
GK17

5J104 AA08 AA11 LA03 LA05 NA05

NA12 NA32 PA14

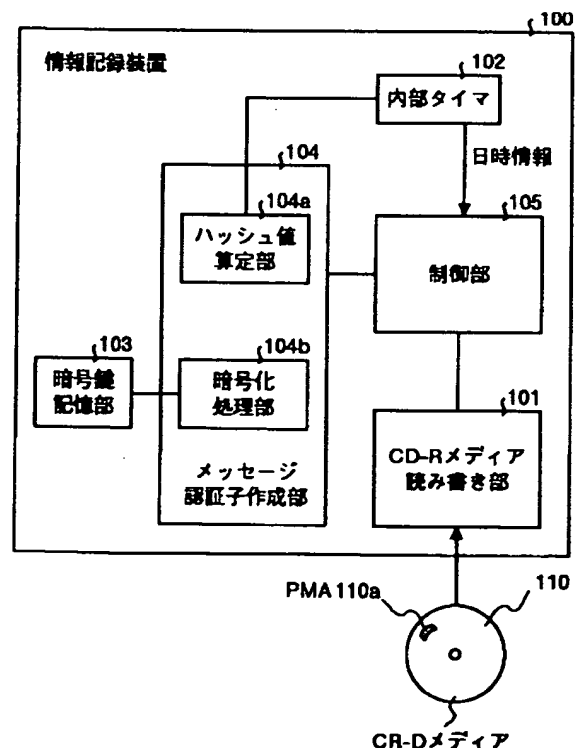
9A001 EE03 FF01 LL03

(54) 【発明の名称】 情報記録装置、真正性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証および記録媒体を提供すること。

【解決手段】 メッセージ認証子作成部104が、PMA110aに保持したベンダーID、ドライブIDおよびディスクIDなどのメディア固有のメディア識別情報と、内部タイマ102が保持する日時情報と、データ記録位置と、電子データとに基づいてメッセージ認証子を作成し、作成したメッセージ認証子を電子データとともにCD-Rメディア110に記録する。



【特許請求の範囲】

【請求項 1】 所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置において、

電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定手段と、前記認証情報算定手段により算定された認証情報を前記電子データとともに情報記録媒体に記録する記録手段と、

前記記録手段によって前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証手段とを備えたことを特徴とする情報記録装置。

【請求項 2】 日時を計時する計時手段をさらに具備し、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報と、前記計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする請求項 1 に記載の情報記録装置。

【請求項 3】 前記認証情報算定手段は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化する暗号化手段を備えたことを特徴とする請求項 2 に記載の情報記録装置。

【請求項 4】 前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定するハッシュ値算定手段をさらに具備し、前記暗号化手段は、前記ハッシュ値算定手段により算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項 3 に記載の情報記録装置。

【請求項 5】 前記暗号化手段は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて前記ハッシュ値算定手段により算定されたハッシュ値を暗号化することを特徴とする請求項 4 に記載の情報記録装置。

【請求項 6】 前記記録手段は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも前記認証情報算定手段が算定した認証情報を記録することを特徴とする請求項 1～5 のいずれか一つに記載の情報記録装置。

【請求項 7】 前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする請求項 1～6 のいずれか一つに記載の情報記録装置。

【請求項 8】 前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判

断することを特徴とする請求項 1～7 のいずれか一つに記載の情報記録装置。

【請求項 9】 前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項 4～7 のいずれか一つに記載の情報記録装置。

【請求項 10】 前記暗号化手段は、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証手段は、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする請求項 9 に記載の情報記録装置。

【請求項 11】 所定の情報記録媒体に記録した電子データの真正性を検証する真正性検証方法において、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定工程と、前記認証情報算定工程において算定された認証情報を前記電子データとともに情報記録媒体に記録する記録工程と、前記記録工程において前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証工程とを含んだことを特徴とする真正性検証方法。

【請求項 12】 前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報と、所定の計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする請求項 11 に記載の真正性検証方法。

【請求項 13】 前記認証情報算定工程は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項 12 に記載の真正性検証方法。

【請求項 14】 前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする請求項 13 に記載の真正性検証方法。

【請求項 15】 前記認証情報算定工程は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて算定されたハッシュ値を暗号化することを特徴とする請求項 14 に記載の真正性検証方法。

【請求項 16】 前記記録工程は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に前記認証情報算定工程で算定した認証情報を記録することを特徴とする請求項 11～15 のいずれか一つに記載の真正性検証

証方法。

【請求項17】 前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする請求項11～16のいずれか一つに記載の真正性検証方法。

【請求項18】 前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項11～17のいずれか一つに記載の真正性検証方法。

【請求項19】 前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする請求項14～17のいずれか一つに記載の真正性検証方法。

【請求項20】 前記認証情報算定工程において、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証工程では、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする請求項19に記載の真正性検証方法。

【請求項21】 前記請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置、真正性検証方法および記録媒体に関し、特に、記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証方法および記録媒体に関する。

【0002】

【従来の技術】 従来、電子データは、その改ざんが容易であり、また完全に消去して証拠隠滅を図ることが容易であるため、かかる電子データは証拠としての価値が低く、証明力が低い。このため、かかる電子データの証明力を高めるためには、電子データにデジタル署名 (digital signature) を施したり、追記型の記憶媒体であるCD-R (compact disc recordable) メディアなどに電子データを格納する必要がある。

【0003】 ここで、このデジタル署名とは、(1) 署名文が第三者によって偽造できないこと、(2) 署名文

が受信者によって偽造できないこと、(3) 署名文を送った事実を送信者が後で否定できないことを要件とするものであり、たとえば公開鍵暗号系では送信者のみが知っている秘密鍵で署名した署名文を相手方に送信することになる。このため、かかるデジタル署名を用いると、署名文によって電子データの証明力が向上する。

【0004】 また、CD-Rのような追記型記憶媒体では、CD-Rメディアに記録した電子データを消去したり改ざんしたとしても、ファイルシステム上で電子データの消去または書き換えがなされたように取り扱われるだけであり、実際には以前の電子データが残留する。このため、かかる追記型記録媒体を用いると、電子データの消去ができないために電子データの証明力が向上する。

【0005】

【発明が解決しようとする課題】 しかしながら、上記デジタル署名は、あくまでもある電子データが特定の送信者 (署名者) によってなされたものであることを証明するためのものであり、かかる電子データを証拠として利用するためのものではない。このため、送信者 (署名者) 自身がある電子データを新たな電子データに置き換えたとしても、たとえ新たな電子データの正当性を確認できても、電子データの証拠性は低下することになる。

【0006】 また、CD-Rのような追記型記録媒体では、確かに一旦CD-Rメディアに書き込んだ電子データを消去することはできないが、この追記型記録媒体に記録した電子データを他の追記型記録媒体に複写する場合に、その一部を複写しないこととすれば、実質的な電子データの改ざんが可能となり、電子データの証拠力を担保することはできない。

【0007】 たとえば、CD-Rメディアに5つのファイルが記録され、そのうちの1つのファイルが不都合である場合には、該当するファイルを除外した4つのファイルのみを他のCD-Rメディアに複写することにより、不都合なファイルを削除したCD-Rメディアを取得できることになる。

【0008】 このように、たとえデジタル署名や追記型記録媒体を用いたとしても、電子データを証拠として用いることは難しいため、かかる電子データの証拠力をいかに高めるかが極めて重要な課題となっている。

【0009】 この発明は、上記問題 (課題) に鑑みてなされたものであり、記録媒体に記録した電子データの証拠力を効率良く高めることができる情報記録装置、真正性検証方法および記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】 上記目的を達成するために、請求項1の発明に係る情報記録装置は、所定の情報記録媒体に電子データを記録するとともに、該記録した電子データの真正性を検証する情報記録装置において、

電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定手段と、前記認証情報算定手段により算定された認証情報を前記電子データとともに情報記録媒体に記録する記録手段と、前記記録手段によって前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証手段とを備えたことを特徴とする。

【0011】この請求項1の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証することとしたので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる。

【0012】また、請求項2の発明に係る情報記録装置は、日時を計時する計時手段をさらに具備し、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報と、前記計時手段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする。

【0013】この請求項2の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定することとしたので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる。

【0014】また、請求項3の発明に係る情報記録装置は、前記認証情報算定手段は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化する暗号化手段を備えたことを特徴とする。

【0015】この請求項3の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することとしたので、認証情報の改ざんなどの不正を防止することができる。

【0016】また、請求項4の発明に係る情報記録装置は、前記認証情報算定手段は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定するハッシュ値算定手段をさらに具備し、前記暗号化手段は、前記ハッシュ値算定手段により算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【0017】この請求項4の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計

時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することとしたので、ハッシュ値という一つの指標を用いて真正性を検証することができる。

【0018】また、請求項5の発明に係る情報記録装置は、前記暗号化手段は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて前記ハッシュ値算定手段により算定されたハッシュ値を暗号化することを特徴とする。

【0019】この請求項5の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化することとしたので、容易に認証情報の復号をおこなうことができる。

【0020】また、請求項6の発明に係る情報記録装置は、前記記録手段は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも前記認証情報算定手段が算定した認証情報を記録することを特徴とする。

【0021】この請求項6の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録することとしたので、情報記録媒体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる。

【0022】また、請求項7の発明に係る情報記録装置は、前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする。

【0023】この請求項7の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体としたので、電子データおよび認証情報のすりかえや削除を防止することができる。

【0024】また、請求項8の発明に係る情報記録装置は、前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【0025】この請求項8の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる。

【0026】また、請求項9の発明に係る情報記録装置は、前記検証手段は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【0027】この請求項9の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる。

【0028】また、請求項10の発明に係る情報記録装置は、前記暗号化手段は、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証手段は、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする。

【0029】この請求項10の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号することとしたので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる。

【0030】また、請求項11の発明に係る真正性検証方法は、所定の情報記録媒体に記録した電子データの真正性を検証する真正性検証方法において、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定する認証情報算定工程と、前記認証情報算定工程において算定された認証情報を前記電子データとともに情報記録媒体に記録する記録工程と、前記記録工程において前記情報記録媒体に記録された認証情報に基づいて前記電子データの真正性を検証する検証工程とを含んだことを特徴とする。

【0031】この請求項11の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証することとしたので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる。

【0032】また、請求項12の発明に係る真正性検証方法は、前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報と、所定の計時手

段が計時した日時情報とに基づいて前記認証情報を算定することを特徴とする。

【0033】この請求項12の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定することとしたので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる。

【0034】また、請求項13の発明に係る真正性検証方法は、前記認証情報算定工程は、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および前記計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【0035】この請求項13の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化することとしたので、認証情報の改ざんなどの不正を防止することができる。

【0036】また、請求項14の発明に係る真正性検証方法は、前記認証情報算定工程は、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定されたハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することを特徴とする。

【0037】この請求項14の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化することとしたので、ハッシュ値という一つの指標を用いて真正性を検証することができる。

【0038】また、請求項15の発明に係る真正性検証方法は、前記認証情報算定工程は、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいて算定されたハッシュ値を暗号化することを特徴とする。

【0039】この請求項15の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化することとしたので、容易に認証情報の復号をおこなうことができる。

【0040】また、請求項16の発明に係る真正性検証方法は、前記記録工程は、前記情報記録媒体の各セクタの一部を形成するサブコード領域に前記認証情報算定工程で算定した認証情報を記録することを特徴とする。

【0041】この請求項16の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録することとしたので、情報記録媒

体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる。

【0042】また、請求項17の発明に係る真正性検証方法は、前記情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体であることを特徴とする。

【0043】この請求項17の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体としたので、電子データおよび認証情報のすりかえや削除を防止することができる。

【0044】また、請求項18の発明に係る真正性検証方法は、前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と前記情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【0045】この請求項18の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる。

【0046】また、請求項19の発明に係る真正性検証方法は、前記検証工程は、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と前記情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には前記電子データが真性であると判断し、両者が一致しない場合には前記電子データが真性ではないと判断することを特徴とする。

【0047】この請求項19の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断することとしたので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる。

【0048】また、請求項20の発明に係る真正性検証方法は、前記認証情報算定工程において、公開鍵暗号系の秘密鍵に応答する公開鍵を前記情報記録媒体に記録し、前記認証工程では、前記情報記録媒体に記録した公開鍵を用いて前記情報記録媒体に記録した認証情報を復号することを特徴とする。

【0049】この請求項20の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号することとしたので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる。

【0050】また、請求項21の発明に係る記録媒体は、前記請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項11～20の動作をコンピュータによって実現することができる。

【0051】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る情報記録装置、情報記録方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。なお、本実施の形態では、情報記録装置としてCD-Rドライブを用いた場合について説明する。

【0052】図1は、本実施の形態で用いる情報記録装置の装置構成を示す機能ブロック図である。図1に示す情報記録装置100は、CD-Rメディア110のPMA (Program Memory Area) 110aに記録したメディア固有のメディア識別情報 () ベンダーID、ドライブIDおよびディスクID) 並びに電子データの先頭アドレス値および日付情報に基づいてメッセージ認証子を算定し、算定したメッセージ認証子を電子データとともにCD-Rメディア110に記録することにより、CD-Rメディアに記録した電子データの証拠力を高めたものである。

【0053】同図に示すように、この情報記録装置100は、CD-Rメディア読み書き部101と、内部タイマ102と、暗号鍵記憶部103と、メッセージ認証子作成部104と、制御部105とからなる。

【0054】CD-Rメディア読み書き部101は、CD-Rメディア110に対する電子データの書き込みと、CD-Rメディア110からの電子データの読み出しをおこなう処理部である。このCD-Rメディア読み書き部101は、CD-Rメディア110に対して電子データを追記的に書き込むことができるが、すでにCD-Rメディア110に書き込んだ電子データを削除することはできない。

【0055】内部タイマ102は、日時情報を常時計数し、計数した日時情報を制御部105からの要求に応じてメッセージ認証部104および制御部105に出力する処理部である。

【0056】暗号鍵記憶部103は、暗号アルゴリズムに対応する秘密の暗号鍵を記憶する記憶部であり、たとえばDES (Data Encryption Standard) 暗号などの慣

用暗号方式を採用する場合にはその秘密鍵を記憶し、RSA (Rivest-Shamir-Adleman) 暗号などの公開鍵暗号方式を採用する場合には、パブリックキーではなくプライベートキーを記憶する。

【0057】なお、この暗号鍵記憶部103に記憶する暗号鍵は、外部から読み出せないよう処理する必要がある。その理由は、かかる暗号鍵を用いて作成するメッセージ認証子は、電子データの真正性を検証するためのものであり、正当な利用者のみが使用すべきものだからである。

【0058】メッセージ認証子作成部104は、電子データとともにCD-Rメディア110に書き込むためのメッセージ認証子を作成する処理部であり、ハッシュ値算定部104aと暗号化処理部104bとを有する。

【0059】ここで、このハッシュ値算定部104aは、CD-Rメディア110に記録する電子データに、ベンダーID、ドライブID、ディスクID、電子データの先頭アドレス値および日付情報を付加したデータ（以下「認証データブロック」と言う。）に、SHA-1やMD5などの所定のハッシュアルゴリズムを適用してハッシュ値を算定する処理部である。

【0060】また、暗号化処理部104bは、暗号鍵記憶部103に記憶した暗号鍵を用いて、ハッシュ値算定部104aが算定したハッシュ値に所定の暗号アルゴリズムを適用して暗号化する処理部である。なお、この暗号アルゴリズムとしては、DES暗号などの慣用暗号系や、RSAなどの公開鍵暗号系を使用することができる。

【0061】制御部105は、情報記録装置100の全体制御をおこなう制御部であり、CD-Rメディア110に電子データを記録する場合には、上記メッセージ認証子作成部104を用いて作成したメッセージ認証子を電子データとともにCD-Rメディア110に格納する。なお、すでにCD-Rメディア110に電子データが記録されている場合には、後述する手順にしたがってかかる電子データの真正性を検証する。

【0062】次に、図1に示す情報記録装置100がCD-Rメディア100へ電子データを記録するデータ記録概念について説明する。図2は、図1に示す情報記録装置100がCD-Rメディア110に記録する記録データのデータ構造の一例を示す図である。

【0063】図2に示すように、通常のCD-Rメディアは、実際に記録する電子データ201と、その電子データ201に係わる制御情報を記録するサブコード202とによって一つのセクタが形成される。なお、かかるサブコード202には、アドレス、コピー情報およびトラフィックタイプなどを記録する領域と予備領域203とからなる。

【0064】このため、この発明に係わる情報記録装置100では、メッセージ認証子作成部104が作成した

メッセージ認証子203aと、このメッセージ認証子203aの作成時に用いた日時情報203bとを上記予備領域203に格納する。

【0065】このように、この情報記録装置100では、CD-Rメディア110の固有の情報をを用いて作成したメッセージ認証子203aを電子データ201とともにCD-Rメディア110に格納することとしたので、電子データ201の証拠力を高めることができる。

【0066】次に、図1に示すメッセージ認証子作成部104によるメッセージ認証子の作成概念について具体的に説明する。図3は、図1に示すメッセージ認証子作成部104によるメッセージ認証子の作成概念を示す図である。

【0067】図3に示すように、かかるメッセージ認証子作成部104では、CD-Rメディア110のPMA110aに記録したメディア固有のベンダーID301、ドライブID302およびディスクID303と、先頭アドレス304および日時情報305とを電子データ306に付加した認証データブロックに所定のハッシュアルゴリズムを適用してハッシュ値307を算定し、暗号鍵記憶部103に記憶した暗号鍵308および所定の暗号アルゴリズムを用いてハッシュ値307を暗号化してメッセージ認証子309を作成する。

【0068】たとえば、RSAなどの公開鍵暗号系を用いる場合には、暗号鍵記憶部103にプライベートキーを記憶しておき、このプライベートキーを用いてハッシュ値307を暗号化することになる。なお、この場合のパブリックキーは、CD-Rメディア110上に記憶してもかまわない。公開暗号系は、パブリックキーからプライベートキーを導出できない暗号系だからである。

【0069】このように、このメッセージ認証子作成部104では、通常CD-RドライブがCD-Rメディア110をフォーマットした時点で必ず書き込むPMA110aから取得したメディア固有のベンダーID301、ドライブID302およびディスクID303などに基づいてメッセージ認証子309を作成しているため、かかるメッセージ認証子309によりCD-Rメディア110は一意に特定できる。このため、CD-Rメディア相互間で電子データが部分複製された場合であっても、このメッセージ認証子309を用いて電子データが真性なものであるか否かを検証することができる。

【0070】なお、PMA110aに記録されたベンダーID301、ドライブID302およびディスクID303が、電子データを記録するCD-Rメディアのものと異なる場合には、電子データの記録を中止するか、または、電子データを記録するCD-Rメディアの認証データブロックに、このベンダーID301、ドライブID302およびディスクID303を追加することにより対応することができる。

【0071】次に、このメッセージ認証子を用いた電子

データの真正性の検証手順について説明する。図4は、図1に示す制御部105によるメッセージ認証子を用いた電子データの真正性の検証手順を示すフローチャートである。なお、ここではすでに電子データがメッセージ認証子とともにCD-Rメディアに格納されているものとする。

【0072】図4に示すように、情報記録装置100は、まず最初に、CD-Rメディア110のPDA110aからベンダーID、ドライブIDおよびディスクIDを取り出し（ステップS401）、該当する電子データとそのメッセージ認証子および日付情報とを取り出す。

【0073】そして、電子データ、ベンダーID、ドライブID、ディスクID、先頭アドレスおよび日付情報からなるデータにハッシュアルゴリズムを適用してハッシュ値を算定し（ステップS402）、このハッシュ値を暗号化してメッセージ認証子を算定する（ステップS403）。

【0074】その後、算定したメッセージ認証子とCD-Rメディア110のサブコード部に記録したメッセージ認証子とを比較し（ステップS404）、両者が一致する場合には（ステップS405肯定）、電子データが真性であるものと判断し（ステップS406）、一致しない場合には（ステップS405否定）、電子データが真性のものではないと判断する（ステップS407）。

【0075】このように、電子データの真正性を検証する場合にも、電子データを記録する場合と同様にしてPMA110aに記憶したベンダーIDなどを用いてメッセージ認証子を作成し、作成したメッセージ認証子をCD-Rメディア110のサブコード部に記録したメッセージ認証子と比較することにより、電子データの真正性を検証することができる。

【0076】なお、電子データの真正性を検証する場合には、電子データを記録する場合と同様にメッセージ認証子を作成するのではなく、サブコード部に記録されたメッセージ認証子を復号し、その復号結果がハッシュ値と一致するか否かによって電子データの真正性を検証することもできる。特に、暗号化処理部104bが公開鍵暗号系のアルゴリズムを使用している場合には、CD-Rメディア110に記憶した公開鍵を用いてメッセージ認証子を復号し、ハッシュ値と照合できるため、メッセージ認証子の生成に使用した暗号鍵を知らなくとも、データの真正性を簡易に検証することができる。

【0077】上述してきたように、本実施の形態では、ベンダーID、ドライブIDおよびディスクIDなどのメディア固有のメディア識別情報に基づいてメッセージ認証子を作成し、作成したメッセージ認証子を電子データとともに記録するよう構成したので、他のメディアに電子データを複写する不正な改ざんを防止することができる。すなわち、CD-Rメディア上のデータをそのま

ま他のメディアに複写したとしても、正規のドライブベンダーから供給されるメディア固有のPMAを複写することはできないため、メッセージ認証子による電子データの真正性を検証することができる。

【0078】また、メディア識別情報だけではなく日付情報をも加味してメッセージ認証子を作成することとしたので、たとえメディア識別情報が正しいCD-Rメディアに複製した場合であってもタイムスタンプが新しくなってしまうため、メッセージ認証子による電子データの真正性を検証することができる。

【0079】なお、ここで注意すべきことは、本実施の形態では、あくまでも電子データの真正性を検証しているのであって、バックアップの作成を否定しているのではないという点にある。あらかじめバックアップメディアを作成した場合には、当然ながらメッセージ認証子の整合はとれないが、このことのみによって直ちに電子データが不正であるわけではなく、証拠力が劣ると認定されるにすぎないのである。

【0080】言い換えると、この情報記録装置100を用いて原本のCD-Rメディアと同じ内容を持つ複製を作成したい場合には、通常の手順と同様にしてCD-Rメディアを複写すれば足りるのである。なお、この場合に複写先で複写の正当性を検証できるように、サブコード部にメディア識別情報（ベンダーID、ドライブIDおよびディスクID）を記録することもでき、その場合には、公開鍵暗号系の暗号アルゴリズムを用いることが望ましい。

【0081】なお、上記実施の形態では、すべてのセクタについてそれぞれメッセージ認証子を作成する場合を示したが、本発明はこれに限定されるものではなく、複数のセクタごとにメッセージ認証子を作成することもできる。この場合には、何セクタ分のメッセージ認証子であるかを示す情報をサブコードの予備領域に記録するとともに、メッセージ認証子を算定する際には複数セクタ分の電子データを1つの電子データとしてまとめる必要がある。

【0082】

【発明の効果】以上説明したように、請求項1の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証するよう構成したので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0083】また、請求項2の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定するよう構成したので、正当な情報記録媒体に複写がお

こなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0084】また、請求項3の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化するように構成したので、認証情報の改ざんなどの不正を防止することができる情報記録装置が得られるという効果を奏する。

【0085】また、請求項4の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化するように構成したので、ハッシュ値という一つの指標を用いて真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0086】また、請求項5の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化するように構成したので、容易に認証情報の復号をおこなうことができる情報記録装置が得られるという効果を奏する。

【0087】また、請求項6の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録するように構成したので、情報記録媒体に係る記録形式を従来のものと変えることなく、効率良く電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0088】また、請求項7の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体とするよう構成したので、電子データおよび認証情報のすりかえや削除を防止することができる情報記録装置が得られるという効果を奏する。

【0089】また、請求項8の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0090】また、請求項9の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、ハッシュ値という指標を用いて効率良く電子データの真正性を

検証することができる情報記録装置が得られるという効果を奏する。

【0091】また、請求項10の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号するよう構成したので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる情報記録装置が得られるという効果を奏する。

【0092】また、請求項11の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報に基づいて認証情報を算定し、算定した認証情報を前記電子データとともに情報記録媒体に記録し、情報記録媒体に記録された認証情報に基づいて電子データの真正性を検証するよう構成したので、情報記録媒体相互間の複写がなされた場合であっても、電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0093】また、請求項12の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報と、計時手段が計時した日時情報とに基づいて認証情報を算定するよう構成したので、正当な情報記録媒体に複写がおこなわれた場合であっても、タイムスタンプにより電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0094】また、請求項13の発明によれば、少なくとも電子データを記録する情報記録媒体に固有の媒体識別情報および計時手段が計時した日時情報を含むデータを所定の暗号アルゴリズムに基づいて暗号化するように構成したので、認証情報の改ざんなどの不正を防止することができる真正性検証方法が得られるという効果を奏する。

【0095】また、請求項14の発明によれば、電子データを記録する情報記録媒体に固有の媒体識別情報、前記計時手段が計時した日時情報、データ記録位置および電子データからなる認証データブロックに対応するハッシュ値を算定し、算定したハッシュ値を所定の暗号アルゴリズムに基づいて暗号化するように構成したので、ハッシュ値という一つの指標を用いて真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0096】また、請求項15の発明によれば、公開鍵暗号系の暗号アルゴリズムおよび所定の秘密鍵に基づいてハッシュ値を暗号化するように構成したので、容易に認証情報の復号をおこなうことができる情報記録媒体が得られるという効果を奏する。

【0097】また、請求項16の発明によれば、情報記録媒体の各セクタの一部を形成するサブコード領域に少なくとも認証情報を記録するよう構成したので、情報記録媒体に係る記録形式を従来のものと変えることなく、

効率良く電子データの真正性を検証することができる情報記録媒体が得られるという効果を奏する。

【0098】また、請求項17の発明によれば、情報記録媒体は、電子データの削除および書き換えができない追記型の情報記録媒体とするよう構成したので、電子データおよび認証情報のすりかえや削除を防止することができる真正性検証方法が得られるという効果を奏する。

【0099】また、請求項18の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たな認証情報を算定し、算定した新たな認証情報と情報記録媒体に記録した認証情報とを比較し、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、認証情報の復号処理を伴うことなく効率良く電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0100】また、請求項19の発明によれば、電子データを記録した情報記録媒体に固有の媒体識別情報に基づいて新たなハッシュ値を算定し、算定したハッシュ値と情報記録媒体に記録した認証情報を復号したハッシュ値とを比較して、両者が一致する場合には電子データが真性であると判断し、両者が一致しない場合には電子データが真性ではないと判断するよう構成したので、ハッシュ値という指標を用いて効率良く電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0101】また、請求項20の発明によれば、公開鍵暗号系の秘密鍵に応答する公開鍵を情報記録媒体に記録し、情報記録媒体に記録した公開鍵を用いて情報記録媒体に記録した認証情報を復号するよう構成したので、公開鍵を用いて効率良く認証情報を復号し、もって効率的に電子データの真正性を検証することができる真正性検証方法が得られるという効果を奏する。

【0102】また、請求項21の発明に係る記録媒体は、前記請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項11～20の動作をコンピュータに

よって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態に係る情報記録装置の装置構成を示す機能ブロック図である。

【図2】図1に示す情報記録装置がCD-Rメディアに記録する記録データのデータ構造の一例を示す図である。

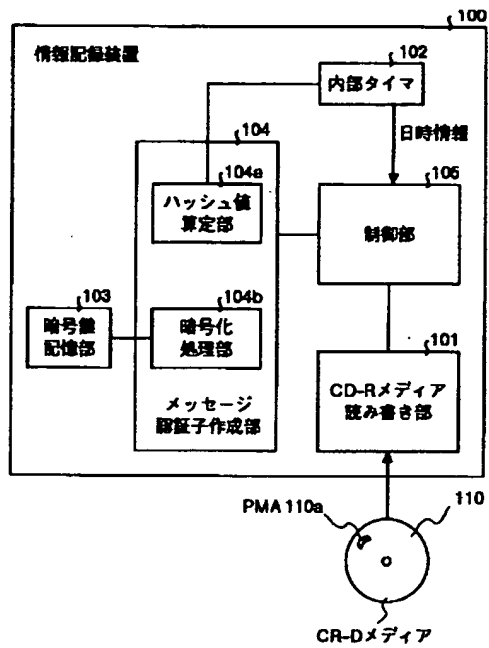
【図3】図1に示すメッセージ認証子作成部によるメッセージ認証子の作成概念を示す図である。

【図4】図1に示す制御部によるメッセージ認証子を用いた電子データの真正性の検証手順を示すフローチャートである。

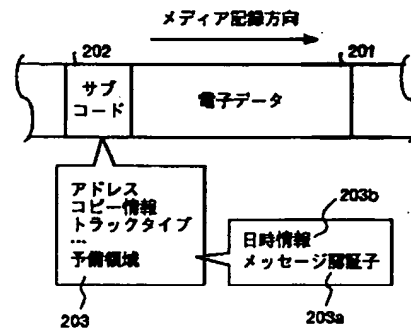
【符号の説明】

- 100 情報記録装置
- 101 CD-Rメディア
- 102 内部タイマ
- 103 暗号鍵記憶部
- 104 メッセージ認証子作成部
- 104a ハッシュ値算定部
- 104b 暗号化処理部
- 105 制御部
- 110 CD-Rメディア
- 110a PMA
- 201 電子データ
- 202 サブコード部
- 203 予備領域
- 203a 日時情報
- 203b メッセージ認証子
- 301 ベンダーID
- 302 ドライブID
- 303 ディスクID
- 304 先頭アドレス
- 305 日時情報
- 306 電子データ
- 307 ハッシュ値
- 308 暗号鍵
- 309 メッセージ認証子

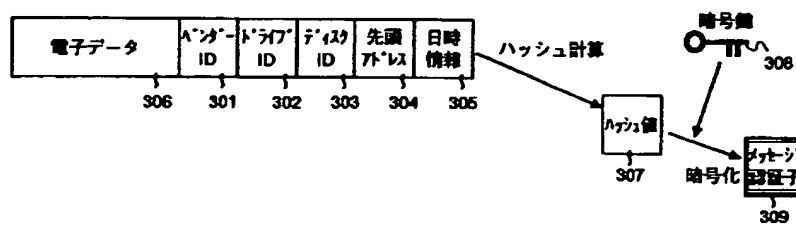
【図1】



【図2】



【図3】



【図4】

